「機能安全」の考え方

安全なシステムへの一歩は「思いやり」から

2006年の組み込みシステムに関係するキーワードは「機能安全」であったようです．確かに，回転扉やエレベータの事故など，工業製品そのものやその後の保守の不具合が相次いで悲惨な結末をもたらすのを見ると，「不具合が発生することを前提として，安全機能を備えることにより不具合の影響を極力低減する」という機能安全の考え方が重要視されるのは当然の流れだと思います注1．

組み込みシステムの障害の原因が，技術者の手抜きであるわけがありません．技術者は，限られた資源（時間・費用）の中で最大限に努力しています．機構設計や回路設計では安全設計が当たり前に行われています．ソフトウェア設計でも，機械制御の分野では，システム・フェイル時の振る舞いとして「殺すな，壊すな」という原則があります．これは，システムに異常が発生しても「第1に人命を優先すること」，「第2に自身を壊さないこと」を原則とした設計を行うことを指します．これは，くしくも，SF作家であるIsaac Asimov氏が自著(1)で述べたロボット3原則の第1条，第3条にそれぞれ相当します（**図1**）．

しかし，直接人命・財産に危害を加えることのないシステムに携わっているソフトウェア技術者は，安全への意識が希薄といわれます．それも仕方のないことかもしれません．なぜなら，ソフトウェアは物理的に存在せず，イメージしにくいため，「ソフトウェア技術者は機械系技術者，電気系技術者，化学系技術者に比べて立体感覚が薄い」(2)からです．とは言え，物理現象と密接な関係にある組み込みソフトウェアがシステムの安全にかかわっていないはずがありません．何かが起こってしまったときに，「ソフトウェア（技術者）だから仕方ない」という言い訳は通用しないのです．

「不具合が発生することを前提として，その影響を極力低減する」ためには，例えば，機能の喪失・劣化を防ぐフォールト・トレラント（耐故障性，耐障害性）の考え方を導入することになります．そのためには，システムそのもののリスクや潜在的リスクを分析し，それぞれに対策を立てることが必要です．システムのリスクを分析する際には，使う人の視点，さらに言うと，使う人を第3者の視点で見ることが重要となります．

「使う人のことを考える」とはどのようなことでしょうか．筆者は，初めての子どもが産まれたときのことを思い出します．生まれて間もないわが子を眺めると気持ちが安らぐ一方で，「この子を危険から守らねばならない」という思いを強くしたものです．自分から動き出さないうちはまだよいのですが，ハイハイしたり，伝い歩きをし始めたりすると，気が気ではありません．子どもの危険になるものはないかと，子どもの視線でものを見るようになりました．すると，ボタンやシャープ・ペンシル，ビデオ・デッキなど，これまでは何とも思っていなかったものが突然「危険なもの」となりました．

子どもが通学するようになると，通学路に危険な個所はないかという観点で見直すことになります．ちょうどこの時期に池田小事件注2があり，安全を地域ぐるみで考える機会がありました．通学路の安全巡視を親（主に母親）たちが行うことになり，「集団で行動する」，「手に何か（護身に役立つもの）を持つ」，「必ず携帯電話を持つ」などを守りながらパトロールを実施しました．これらも，女性の視点でパトロールを計画したことによって出てきたアイデアです．

安全な製品を作る（リスクを低減する）ための分析においては，製品を使う人の立場や観点に立ち，観察したり想像したりすることが大事でしょう．そのために必要なのは「思いやり」だと思います．例えば，使う側の無知から発生する問題までをもあらかじめ想定し，特定の操作しかできないように，あるいは危険な操作をしにくいようにユーザ・インターフェースを改善するといった対応が必要になるでしょう．

注1：「機能安全エキスパートセミナー」に関する組み込みネットのレポートを参照（URLはhttp://www.kumikomi.net/article/report/2006/26f_safe/01.html）．

注2：2001年6月に起こった無差別殺傷事件．大阪教育大学附属池田小学校に男が侵入し，児童8名を殺害，児童13名と教師2名に傷害を負わせた．

第1条　ロボットは人間に危害を加えてはならない．また，その危険を看過することによって，人間に危害を及ぼしてはならない．
（A robot may not harm a human being, or, through inaction, allow a human being to come to harm.）
第2条　ロボットは人間に与えられた命令に服従しなければならない．ただし，与えられた命令が，第1条に反する場合は，この限りでない．
（A robot must obey the orders given to it by the human beings, except where such orders would conflict with the First Law.）
第3条 ロボットは，前掲第1条および第2条に反するおそれのない限り，自己を守らなければならない．
（A robot must protect its own existence, as long as such protection does not conflict the First or Second Law.）

図1　ロボット3原則

参考・引用*文献

(1)* Isaac Asimov；われはロボット，早川書房，1983年．
(2)* 松原友夫；永続する品質改善へ向けて，ソフトウェアテストシンポジウム（JaSST）2006 大阪 基調講演，http://www.jasst.jp/jasst06w/pdf/A1.pdf

しゅくぐち・まさひろ
三菱電機マイコン機器ソフトウエア（株）